UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/624,344	07/22/2003	Jeffrey S. Bardsley	5577-265	7591

20792   7590   12/27/2007

MYERS BIGEL SIBLEY & SAJOVEC
PO BOX 37428
RALEIGH, NC 27627

EXAMINER
HOMAYOUNMEHR, FARID

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
12/27/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

MAILED

DEC 2 7 2007

Technology Center 2100

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Application Number: 10/624,344
Filing Date: July 22, 2003
Appellant(s): BARDSLEY ET AL.

D. Randal Ayers
Registration No. 40,493
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 10/15/2007 appealing from the Office action

mailed 7/25/2007.

(1) Real Party in Interest

The statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The statement of the status of related appeals and interferences contained in the brief is correct.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct. The changes are as follows: Claims 18-23 are rejected as nonstatutory under 35 USC 101.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Following documents were relied upon in rejection of claims:

| 2003/0084349 | Friedrichs | 08-2002 |
| 2003/0004689 | Gupta | 06-2002 |

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 101

Claims 18-23 rejected under 35 U.S.C. 101 because the claimed invention is

directed to non-statutory subject matter. The claimed invention does not fall within at

least one of the four categories of patent eligible subject matter (process, machine,

manufacture, or composition of matter). The claimed invention is a data structure, which

is neither a method nor a manufacture. The recitations of "computer readable field" does

not provide a manufacture that would provide the necessary structure and functionality

for the invention to fall within one of the statutory categories.

Claim Rejections - 35 USC § 103

Claim 1-23 rejected under 35 U.S.C. 103(a) as being unpatentable over

Friedrichs et al. (U.S. Patent Application Publication No. 2003/0084349 A1, filed August

9, 2002), and further in view of Gupta et al. (U.S. Patent Application Publication No.

2003/0004689 A1, filed June 13, 2002).

9.4.1. As per claim 1, Friedrichs and Gupta are directed to a method of generating

computer security threat management information (Friedrich paragraph 8-10),

comprising: receiving notification of a computer security threat (Friedrich paragraph 40

to 44 or 20-30); generating a computer-actionable Threat Management Vector (TMV)

that is suitable for use by an automated threat management system from the notification

that was received (as described in Friedrich paragraphs 17-20, security event data is

collected from all network devices, and stored in fields of a database. The Extractor 120

performs analysis on data and stores the analysis result in the upload server or the

database server (parag. 20). In addition, Friedrich paragraphs 30-45 teach database

server 230 supplementing demographic and geographic information regarding the

network generating the security events (parag. 30 and 35), identifying and storing

validated security threats based on security event data (parag. 37), the All Events

database, which includes all security events (parag. 40-41) and Product database 450,

which includes information about specific products that exhibit vulnerabilities, product

version information, and details about how to patch a flaw, or other security measures

that a network operator could implement, and how to repair a damage (parag. 45). All

the mentioned data and databases are combined in a single database such as Threat

database (parag. 46). Therefore, the Threat database contains a set of fields related to

a security threat and its associated data.), the TMV including therein a first computer-

readable field that provides identification of at least one system type that is affected by

the computer security threat (per Friedrich paragraph 42, information stored in

databases and included in the analysis and report includes demographic data. Per

paragraph 35, the demographic data includes type of network and Operating System), a

second computer-readable field that provides identification of a release level for the

system type (per Friedrich paragraph 42, the proprietary information of security devices

are included in the databases for analysis and report, in addition to demographic

information, which shows detailed specifications of systems involved in the security

threat are completely collected in the databases. Also note that the version information

of the products is stored in Product database (Friedrich parag. 45)), and a third

computer-readable field that provides identification of a set of possible countermeasures

for a system type and a release level (Friedrich paragraph 45);

As discussed above, Friedrichs teaches creation of a database including relevant

information for detection and mitigation of attacks. Friedrich also teaches reporting the

data for analysis, for example, by network administrators, but it does not explicitly teach

transmitting the computer-actionable TMV (a data structure, such as a file) that is

generated to a plurality of target systems for processing by the plurality of target

systems.

Gupta is directed to a system for provisioning computers against computer attacks,

which includes, constructing a hierarchy of attacks and countermeasures, identifying

attacks and associated detection and protection measures, and downloading the

detection and protection measures to the target platform (Abstract). As indicated in Fig.

15- 17, and paragraphs 164 to 165, a data structure containing all information such as

what attacks a given environment is vulnerable to, what protection means are available,

and how detection alerts are correlated is created. The detection and protection

measures are put in an attack file, and downloaded to the target systems for detecting

and mitigating attacks. Therefore, Gupta teaches creation of a data structure, such as a

file, that can be downloaded to the systems to be protected (target systems), such that

the target system would mitigate the attacks based on the downloaded file.

Gupta and Friedrichs are clearly directed to analogous arts. At the time of invention, it

would have been obvious to the one skilled in art to use Friedrich's system, which

collects, generates, and store threat management information in a data structure, and

modify it, according to Gupta's teachings, to create an attack file including the threat

management information and the mitigation information, and send the attack file to

target systems to mitigate the attacks associated with the threats.

The motivation for combination is creating a system that gathers all required information

to create effective countermeasures, and deploys the created countermeasures to

mitigate attacks. Friedrich paragraph 5-7 indicates the purpose of tying together

information gathered from different devices, and aggregating information about network

traffic, analyzing it to identify treats, and distributing it to neutralize the attack. Gupta

paragraph 7-9 motivates and creates a single platform that gathers and uses all relevant

data to produce provisioning data (attack file), which is downloaded to target systems to

effectively mitigate attacks.

9.4.2. As per claim 2, Friedrichs is directed to a method according to claim 1 wherein

the generating comprises selecting a system type, release level and possible

countermeasures from a database that lists system types, release levels and possible

countermeasures in a computer-readable format (Friedrich paragraphs 40-45, and

paragraph 46 showing all mentioned databases could be combined to one database).

9.4.3. As per claim 3, Friedrichs is directed to a method according to claim 1 wherein

the system type comprises a computer operating system type and wherein the release

level comprises a computer operating system release level (Friedrich paragraph 35, 45,

and 42).

9.4.4. As per claim 4, Friedrichs is directed to a method according to claim 1 wherein

the set of possible countermeasures comprises an identification of a countermeasure

mode of installation (Friedrich paragraph 45 teaches including details about how to

patch a flaw and security measures to mitigate a flaw. Examiner takes the official notice

that installation mode (binary, manual, URL, local or server) is one of the details

necessary to know when installing a patch, and therefore would have been obvious to

the one skilled in art).

9.4.5. As per claim 5, Friedrichs is directed to a method according to claim 1 wherein at least one of the identifications comprises a pointer (Examiner takes the official notice that pointers are broadly used in databases to identify data. Therefore, it would have been obvious to use a pointer for identification of data).

9.4.6. As per claim 6, Friedrichs is directed to a method according to claim 1 wherein the TMV further includes therein a fourth computer-readable field that provides identification of at least one subsystem type that is affected by the computer security threat and a fifth computer-readable field that provides identification of a release level for the subsystem type, the third computer-readable field providing identification of a set of possible countermeasures for a subsystem type and a release level (per paragraph 22, the Security Device 110 gathers details of elements participating in the threat. The details include ports, which is a subsystem if a network element. In addition, Hunter server 140 gathers further details such as IP address of system. As described in response to claim 1, the version level of subsystems are also collected and reported as the comprehensive data about systems participating in the threat are recorded and reported).

9.4.7. As per claim 7, Friedrichs is directed to a method according to claim 6 wherein the subsystem type comprises an application program type (paragraph 35).

9.4.8. As per claim 8, Friedrichs is directed to a method according to claim 1 wherein

the TMV further includes therein a sixth computer-readable field that provides

identification of the computer security threat (per paragraph 43, Vendor signature

databases contain a listing of all known security event types for a particular vendor, and

therefore identifies the threats).

9.4.9. Limitations of claims 9 and 10 are substantially the same as claim 1 above.

9.4.10.   As per claim 11, Friedrichs is directed to a system according to claim 9

further comprising a common semantics database that lists system types, release levels

and possible countermeasures in a computer-readable format (Fig. 4 and associated

text), wherein the TMV generator is responsive to the common semantics database to

generate the TMV based upon user selection of a system type, release level and

possible countermeasures from the common semantics database for the computer

security threat (generation of a report based on user defined parameters was a well-

known feature of database management systems at the time of invention).

9.4.11.   Claims 12 to 23 are substantially the same as claims 1-8 above.

(10) Response to Argument

In response to claim rejections under section 103, based on Friedrichs (US

Patent Application Publication No. 2003/0084349), and Gupta (U.S. Patent Application

Publication No. 2003/0004689), the appellant has argued that the combination does not

make the claim limitations obvious. The following describes Appellant's specific

arguments and the corresponding responses:

A.   Introduction

In this section the appellant makes a general statement that the cited prior art is simply

another example of labor-intensive prior art security threat management system

described in the background of their application. Appellant does not discuss any specific

claim limitations, or how the claims distinguish the invention from the prior art in this

section.

B.   The rejections of claims 1, 7-10 and 16-17

B.1.   With respect to claim 1, appellant argues:

   a.   Friedrichs Does Not Disclose a TMV Having a Field Identifying at Least

One System that is Affected by the Security Threat.

Specifically, appellant argues: "However, what the cited portion of Friedrichs discloses is a

Sensors database 405 that contains demographic information about the location, type and/or

operating system of the security devices that uploaded information into the All-Events database

or reported the security event. (Friedrichs at [0042])". It appears that appellant argues that

the demographic information only includes the type of system that reported the security

event, and not the system that is affected by the security event.

However, appellant does not mention the cited paragraph 35, and paragraph 34 of

Friedrichs, wherein the relative part reads:

[0034] Security Event Collection step 310 may <u>also include obtaining demographic and</u>

*<u>geographic information regarding</u> **the network providing security event data.** In an*

embodiment, the demographic and geographic information for a network is stored

ahead of time in a database. The stored demographic and geographic information can

then be used to supplement the security event after it is collected. In another

embodiment, security events are mapped to the database entry for the appropriate

network. <u>In yet another embodiment, demographic and geographic information may be</u>

<u>provided by the security device recording the security event, such as by including the</u>

<u>information as fields within the security event.</u> Other examples of how to associate

demographic and geographic information with a security event will be apparent to those

skilled in the art.

[0035] Many types of information may be included in the demographic and geographic

information associated with a security event. <u>For example, the demographic information</u>

*<u>may include the</u> **type of network reporting the security event**, the applications or*

operating systems in communication with the network, or the types of security measures

implemented on the network.

Therefore, Friedrichs clearly teaches demographic information, which includes the type

of system that is affected by the security event.

> b.   Friedrichs Does Not Disclose a TMV Having a Field Identifying a Release
> Level for the System Type Affected.

Appellant makes a similar argument to the one in section "a" above with respect to the

field containing the Release Level of the system affected by the security event.

Specifically, applicant argue that Friedrichs teaches a field containing Release Level of

the reporting device, and not the that of the affected system device. However, Friedrichs

cited paragraph 45 reads:

[0045] The entries in Common Signature database 430 are also linked to Vulnerability

database 440 and Product database 450. Vulnerability database 440 contains a listing

of validated security threats, such as software flaws that are susceptible to attack via

network. Product database 450 contains a listing of specific products that exhibit a

particular vulnerability. For example, Vulnerability database 440 may contain an entry

describing a particular way that SNMP software may be exploited. This entry would

describe the flaw in detail, including how the flaw may be exploited and what type of

harm could result from an attack targeting this flaw. Product database 450 would then

have one or more entries containing vendor, product, and version information for

products that are vulnerable due to this flaw in SNMP.

Therefore, Friedrichs teaches entries (fields) that indicate the version information

(Release Level) of the products that are vulnerable, and therefore the subject of the

security event. Note that all this information is stored in an AllEvents database as

described in paragraphs 40 and 41. Therefore, Friedrichs gathers and stores all the

information required by the claim language.

Appellant further argues: "In fact, the *Office Action* implicitly concedes as much by stating that

Friedrichs "shows detailed specifications of systems involved in the security threat", where what

Claim 1 recites is that the second field identifies the system type of the system that is affected by

the threat. *(Office Action* at 9, emphasis added)." However, it is not clear what appellant

means by "the Office action concedes". The complete statement referred to by the

appellant is as follows:

"per Friedrich paragraph 42, the proprietary information of security devices are included

in the databases for analysis and report, in addition to demographic information, which

shows detailed specifications of systems involved in the security threat are completely

collected in the databases. Also note that the version information of the products is

stored in Product database (Friedrich parag. 45)". Friedrich stores information relative to

the systems involved in the security event, which includes the systems affected by the

security event. As mentioned above, the Release Level of the systems affected by the

system is explicitly mentioned and included among the collected data.

Appellant further argues that the "release" information is not provided by Friedrichs.

However, as mentioned in the above, Friedrichs clearly teaches storing and using the

version of the software products that are subject of a security event. The release

information is equivalent to software version. Appellant has not identified any specific

definition of the "release" information that is distinguished from the version of the

software.

c.   Gupta Does Not Disclose Generating a Computer Actionable

TMV that is Transmitted to a Plurality of Target Systems

Appellant argues: "In particular, the cited portion of Gupta discusses downloading an "attack

file 149" to a sensor management system 26. However, as made clear by Gupta, the sensor

management system 26 is not the "target system." (Gupta at 0164, stating "A sensor is then

supplied, through a download, with the protective software (e.g., the attack tile) for the target

platform). Instead, as shown in Fig. 1 of Gupta, the sensor management system 26 is part of a

sensor module 27 that is interposed between the target system (i.e., protected server 32) and the

enterprise network 30." It appears that the appellant argues that the attack file (TMV) is

only transmitted to the sensor management system (SMS). However, Gupta teaches a

Sensor Management System (SMS) and sensors (see Fig. 1 and associated text),

which are different entities. As described by Gupta paragraph 164, the attack file is

supplied (transmitted) to the sensors, which are entities different than the SMS. The

sensors perform attack mitigation via item 54 as described, for example, in Gupta

paragraph 87 (note that as shown in Fig. 2, item 54, which performs attack mitigation, is

part of the sensor). The sensors are associated with target platforms, as indicated in

paragraph 164 and the abstract. Therefore, Gupta teaches transmitting the attack file

(TMV) to target systems (sensors). Note also that the claim language does not require

the target system and the system affected by the threat to be the same. Also note that a

sensor associated with a target platform is part of the target system, as a system

pertains to a combination of elements associated and working together.

Therefore, Gupta clearly teaches transmitting an equivalent of the TMV to a plurality of

target systems as required by the claim.

Applicant further argues that there is no indication that the attack file is computer

actionable, citing paragraph 151 of Gupta. However, Gupta paragraph 151 reads:

[0151] The secure update download module 148 includes executable code to

download an attack file 149 to a sensor management system 26. The attack file

149 specifies attacks and ***counter measures.*** *Preferably, the file also*

identifies unknown attacks and suggests responses for such attacks. The attack

file 149 includes information forming the intrusion signatures 70 processed by

the classification and pattern-matching module 68.

As shown in the above, the attack file includes countermeasures. In addition, paragraph 87 clearly shows that the system performs actions to mitigate attacks, such as terminating TCP connections. Moreover, paragraph 165 states processes for utilizing this representation constitute effective methods for operation and deployment of solutions.

Note further that, as indicated in Friedrichs paragraph 8, the security information relative to the threats (TMV) gathered by Friedrichs is generated by a computer and sent to a processor for analysis. Therefore, Freidrichs' reports (TMV) are computer-actionable. In addition, since the threat related data is sent to a processor for analysis, it is suitable for use by an automated threat management system, as the processor is generally part of a computer and a computer automatically analyzes the data. Also see paragraphs 25 and 33 as examples to show that the threat related data analysis is performed by processing (compute) systems. Therefore, Friedrichs discloses a report (TMV) that is computer actionable and suitable for use by an automated threat management system.

In addition to the above, appellant has not identified any specific definition of "computer-actionable" item that sets it apart from a collection of data fields. In the most general sense, even a group of fields are computer-actionable, as a computer acts on the fields (reads, writes, or changes). Note further that claim 1 does not identify anything beyond a group of fields containing data for the TMV. Also note that appellant's Specification at Fig. 3 shows generation of a computer-actionable item, which is gathering a notification

of security threats and generating a TMV. As shown in Fig. 4 and paragraph 45 of the

appellant's Specification, The TMV is a collection of data fields.

Appellant further argues: "Likewise, Gupta expressly states that two of the ways that the

attack file 149 may be delivered are by e-mail alerts and SMS alert notifications. (Gupta at

0152). These methods of delivery would generally not result in automatic processing of the

attack file, further making clear that the attack file 149 is in the form of, for example, a report,

which is no different than the type of information that is provided to the target systems of

Friedrichs, and which certainly is not the "computer actionable" file recited in Claim 1."

It appears that appellant is attempting to argue that since the attack file is transmitted

via email, it cannot be automatically processed. However, the cited paragraph 152

reads:

[0152] The attack file 149 can be downloaded using different approaches. The

secure update download module 148 can periodically download the attack file

149. Alternately, the secure update download module can download the attack

file 149 in response to a request from a sensor management system 26.

Alternately, email alerts may also be used to deliver updated attack files 149.

The SMS alert notification module 152 may be used to send alerts by secure

e-mail (e.g., SMIME) when a new signature update is available for download.

Based on the above, the attack file is downloaded via different approaches, not limited to email or SMS. In addition, email is well capable of transmitting items capable of performing a computer action, such as software. Therefore, the fact that Gupta suggests ways to transmit the attack file (email or the other) has absolutely no bearing on whether the attack file can be automatically processed or not.

Based on the discussion above, none of the applicant's arguments traversing the rejection of claim 1 are persuasive.

B.2.   With respect to claims 7-10 and 16-17, appellant's argument is based on their dependency on claim 1. However, as discussed above, their argument relative to allowability of claim 1 is non-persuasive.

C.   The rejection of claim 2

Appellant argues that the cited portions of Friedrichs do not teach the limitations for two reasons. First, the appellant argues that the cited portions do not show converting the information into a computer-actionable format. However, this requirement is not found in the claims at hand. In fact, the word "converting" does not appear in claim 2. As mentioned in the above, Friedrichs creates the required data fields and stores them in databases.

Second, the appellant argues that the cited portions are discussing information in the

databases, as opposed to generating a TMV and transmitting it to target systems.

However, generation of TMV and transmission to target systems are shown in rejection

of claim 1, and its associated discussions. The additional limitations of claim 2 are

related to selecting the data fields from a database, which is addressed by the rejection

of claim 2.

D.   The rejection of claim 3

The release level information is equivalent to software version. Appellant has not

identified any specific definition of the "release level" information that is distinguished

from the version of the software.

Therefore, the "release level" information is taught by Friedrichs.

E.   The rejection of claim 4

Appellant argues, once again, that the information in the Product database is not in

computer-actionable format. However, as discussed above, per Friedrichs paragraph 8,

the security information relative to the threats (TMV) gathered by Friedrichs is

generated by a computer and sent to a processor for analysis. Therefore, Freidrichs'

reports (TMV) are computer-actionable. In addition, since the threat related data is sent

to a processor for analysis, it is suitable for use by an automated threat management

system, as the processor is generally part of a computer and a computer automatically

analyzes the data. Also see paragraphs 25 and 33 as examples to show that the threat

related data analysis is performed by processing (computer) systems. Therefore,

Friedrichs discloses a report (TMV) that is computer actionable and suitable for use by

an automated threat management system.

In addition to the above, appellant has not identified a specific definition of "computer-

actionable" item that sets it apart from a collection of data fields. In the most general

sense, even a group of fields are computer-actionable, as a computer acts on the fields.

Note further that none of the claims identifies anything beyond a group of fields

containing data for the TMV. Also note that appellant's Specification at Fig. 3 shows

generation of a computer-actionable item, which is gathering a notification of security

threats and generating a TMV. As shown in Fig. 4 and paragraph 45 of the appellant's

Specification, the TMV is a collection of data fields.

Applicant also states, it is clear that the information in the Products database is not part

of the report, but the appellant provides no reason to support that statement.

Appellant further argues: "Appellants respectfully submit that there has not been, nor can there

be, a showing that it would have been obvious to include the mode of installation information in

a specific field of a computer actionable TMV as recited in Claim 4." However, appellant

states no reason to support their statement. In fact, the mode of installation (binary,

manual, URL, local or server) is an essential element for installing a patch or a software.

This information is typically accompanied with the software or patch so that the

installation would be successful. In addition, it is clear that the "mode of installation" is

not the subject matter of the invention. A person skilled in art would have found it

obvious to include that information when a software or a patch installation is necessary.

F.   The rejection of claim 5

Appellant's argument, once again, is based on a data field and its inclusion in the TMV

in a computer-actionable format. However, as discussed above, inclusion of different

data fields in the TMV in a "computer-actionable" is generally taught by Friedrichs.

Unless it is shown that inclusion of a "pointer" data field creates an unexpected result, it

would have been obvious to include a pointer in a TMV, in a computer-actionable format

as discussed above.

G.   The rejection of claim 6

Appellant argues: "The *Office Action* states that the description of the Security Device 110 and

Hunter server 140 in paragraph [0022] of Friedrich discloses the recitations of Claim 6. *(Office

Action* at 7 and **10-11).** Notably, the *Office Action* does not even attempt to explain how these

devices of Friedrichs correspond to the recitations of Claim 6, and Appellants respectfully submit

that no such explanation could be provided." However, Examiner rejection of claim 6 does

provide a thorough explanation of how the cited portion meets the requirements of claim

6 (see Non-Final Office action, dated 7/25/2007, at section 7.6.). As indicated in the

Officer Action, per paragraph 22, the Security Device 110 gathers details of elements

participating in the threat. The details include ports, which is a subsystem if a network

element. In addition, Hunter server 140 gathers further details such as IP address of

system. As described in response to claim 1, the version level of subsystems are also

collected and reported as the comprehensive data about systems participating in the

threat are recorded and reported.

H.   The rejection of claim 11

Appellant argues; "The *Office Action* takes the position that Fig. 4 of Friedrichs and associated

text discloses "a common semantics database that lists system types, release levels and possible

countermeasures in a computer-readable format." *(Office Action* at 9). Appellants respectfully

submit, however, that this is not the case." Therefore, appellant simply argues that the cited

portion of Friedrichs does not teach the requirements, without discussing the merits of

the cited portions. However, the cited portions include, for example, paragraph 45,

which shows that the databases and their data records are linked to one another. This

shows a common semantic database. The other requirements of the claim, such as the

contents of the data fields, i.e. the system type, release level, and possible counter

measures are also taught by Friedrichs, as indicated by claims 1-9 and other related discussion. Therefore, Friedrichs does teach all the elements of claim 11.

Applicant further argues: "More importantly, Friedrichs clearly does not disclose making a TMV generator... responsive to the common semantics database" as recited in Claim 11." However, as discussed in the rejection of claims 1-9 and other associated discussions in the above, Friedrich teaches generation of TMV, which is based the collective information and stored in the databases, and most notably the Threat database 460, which based on paragraph 0046, includes all information stored in all different databases, and therefore includes all the data fields identified and gathered by Friedrichs system.

Sections I to R.

In sections titled from I to R, appellant argues that claims 11-15, 18-23 are allowable because they are dependent on claims which are allegedly allowable. However, as discussed above, none of the mentioned claims are allowable.

Note once again, there appears to be no argument relative to rejection of claims 18-23 under 35 U.S.C. 101, as outlined in the Office Action dated 7/25/2007.
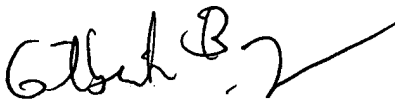
Based on the above, applicant's argument relative to the allowability of claims is found

non persuasive, and the rejections should be sustained.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the

Related Appeals and Interferences section of this examiner's answer.

Respectfully submitted,

/Farid Homayounmehr/
Farid Homayounmehr
Examiner, GAU 2132

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

December 18, 2007

Conferees:

Gilberto Barron Jr
SPE 2132

/Benjamin Lanier/
Benjamin Lanier
Primary Examiner
Art Unit 2132